REMARKS

Claims 1-31 are pending in the above-referenced patent application. The Examiner has maintained his rejection under 35 USC 103. He therefore issued a Final Office Action, dated September 28, 2005, rejecting all of the pending claims. He maintained his position regarding the claims in an Advisory Action, dated December 20, 2005. It is noted that the Advisory Action refers to claims 1-13 as being rejected; however, this is believed to be a typographical error.

Assignee continues to traverse the Examiner's rejection of claims 1-31. A basis for this traversal is described in more detail below; however, Assignee also maintains that many other additional reasons for traversing the Examiner's position exist. The discussion below, however, is believed to be more than sufficient to overcome the Examiner's rejection of the pending claims.

The basis for the Examiner's rejection is 35 USC 103(a). The Examiner relies upon Wright (USP 6,052,466; hereinafter, Wright) and further in view of Nakamura (USP 5,159,633; hereinafter, Nakamura) and Coppersmith et al. (USP 6,192,129; hereinafter Coopersmith).

Assignee specifically reminds the Examiner that, based upon the MPEP:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. MPEP §2142 and §2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Assignee's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the inventor has done. "To support the conclusion the claimed invention is directed to obvious subject matter, either the references expressly or implicitly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why an artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App.& Inter. 1985).

Beginning with claim 1, as an example, Assignee believes that many reasons exist for asserting that the proposed combination would fail to render claim 1 unpatentable. For example, assuming,

simply for the sake of legal argument, and not conceding, that the documents cited by the Examiner were capable of being properly combined, this combination would still fail to produce claim 1 because the combination does not teach or suggest all of the limitations of claim 1. For example, claim 1 specifically recites:

> "...;
> generating in real time a second deciphering round key based on said generated first deciphering round key while said incremental deciphering for a first round is being performed;
> ... .

None of the documents, whether considered individually or in combination, suggests or discloses this aspect of the recited claim. It is asserted that the Examiner has failed to show how the cited documents, whether considered individually or in combination, disclose or even suggest this aspect of claim 1.

In particular, the Examiner relies heavily upon Wright. However, as has been previously pointed out, Wright is not relevant to block ciphers and does not teach or suggest technology related to such ciphers. Wright through the document refers to "cipher streams." See, for example, col. 4, lines 10-30. However, cipher streams to do not employ round keys. Round keys are employed in connection with block cipher mechanisms, which, again, are not taught or suggested by Wright. Thus, Wright could not and does not teach or suggest the limitations recited above of claim 1, as an example.

A similar comment has been made previously and is repeated here regarding Nakamura. Nakamura does not teach or suggest technology related to block ciphers. For example, Nakamura states, at col. 7, lines 10-13: "The key is changed for each communication....." Again, this is not employing round keys, such as where, for example, a full block of text is encrypted before a key is

changed. Rather, this refers to a cipher stream approach. Thus, Nakamura also could not and does not teach or suggest the limitations recited above of claim 1, as an example.

Finally, Coopersmith does not cure the deficiencies described above with respect to Wright and Nakamura. Thus, while Coopersmith does describe block ciphers and round keys, Coopersmith does not teach or suggest any of the other limitations recited above, for example. The Examiner specifically points to col. 7, lines 48-59; col. 1, lines 60-65; and col. 2, lines 31-40 of Coopersmith; however, none of these portions of the document teach or suggest, for example, generating in real time a second deciphering round key based on a generated first deciphering round key while incremental deciphering for a first round is being performed, as is recited, for example, in claim 1.

While Assignee believes that the foregoing is more than sufficient to overcome the Examiner's rejection of claim 1 under 35 USC 103; Assignee would also like to repeat the following point also made in previous responses: one of ordinary skill in the art would also not be motivated to make the asserted combination in the first instance. As mentioned above, Wright and Nakamura do not teach or suggest block ciphers. In contrast, Coopersmith does describe block ciphers. Therefore, the combination asserted by the Examiner would, in effect, destroy the security advantages, and also potentially the entire functionality, of employing a cipher stream, as is described in Wright and Nakamura, for example. For at least these reasons, one of ordinary skill in the art would not be motivated to make the proposed combination.

Thus, for at least the foregoing reasons, it is respectfully requested that the Examiner at least withdraw his rejection of claim 1.

Furthermore, the remaining rejected claims, 2-31, patentably distinguish from the cited documents for at least the same or similar reasons as described above. These remaining claims either depend from claim 1 or these claims contain limitations similar to the limitations of claim 1, such as claims 10 and 21, for example.

It is likewise noted that the addition of Adler (USP 4,255,811; hereinafter, Adler) to the combination of Wright, Nakamura, and Coopersmith in order to reject claims 9, 19 and 30 also does not cure the deficiencies noted above. Adler does describe block ciphers. Thus, the Examiner, has pointed to, for example, col. 3, lines 36-47; col. 3, lines 49-51; and col. 3, lines 65-67 through col. 4, lines 1-9. However, none of these portions of the document teach or suggest the limitations of claims 1, 10 or 21, for example. Since claims 9, 19 and 30 depend from such claims, claims 9, 19 and 30 distinguish on at least the same basis. Therefore, it is respectfully requested that the Examiner withdraw his rejection of all the remaining claims, claims 2-31, as well.

CONCLUSION

In view of the foregoing, it is respectfully submitted that all of the claims pending in the above-referenced patent application are in condition for allowance. If the Examiner has any questions, he is invited to contact the undersigned at (503) 439-6500. Reconsideration of this patent application and early allowance of all the claims is respectfully requested.

Please charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account number 50-3703.

Respectfully submitted,

Howard A. Skaist, Reg. No. 36,008

Dated: 2/28/06

Berkeley Law & Technology Group, LLC
1700 NW 167th Place, Suite 240
Beaverton, Oregon 97006
503.439.6500